

On Premise: Opsætning af AD FS

Formål

Dette dokument vejleder i opsætningen af Active Directory Federation Services (AD FS) til Single Sign-On på jeres On-Premise-installation.

Hvis I ønsker hjælp til opsætningen af AD FS, men det ikke er en del af jeres implementering, bedes I kontakte support@xflowsupport.dk.

Forarbejde

- I opstartsblanketten skal I vælge, at I ønsker at benytte jer af AD FS
- I skal bruge jeres AD FS metadata URL (det er ofte i stil med <https://adfs.eksempel.dk/federationmetadata/2007-06/federationmetadatan.xml>), som skal indtastes i blanketten
- I skal sørge for, at webserveren kan kontakte jeres AD FS server. For SaaS kunder skal jeres AD FS løsning være åben mod internettet. *Se Microsofts dokumentation for opsætning af en AD FS server proxy. Du må aldrig åbne en AD FS server direkte mod internettet!*

Vejledning

- I skal tilføje XFlow som Relying Party Trust i jeres AD FS ved at tilføje adressen på jeres XFlow-installation. Adressen er <https://eksempel.dk/FederationMetadata/>, hvor eksempel.dk er adressen

på jeres XFlow-installation

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options:

- Import data about the relying party published online or on a local network**
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file**
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:
- Enter data about the relying party manually**
Use this option to manually input the necessary data about this relying party organization.

At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

- Jeres trust skal oprettes, så det benytter e-mail claim. Det kan se ud som nedenfor, men vær opmærksom på, at det kan se forskelligt ud fra system

til system.

Edit Rule - AD

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
AD

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

View Rule Language... OK Cancel

- Når ovenstående er oprettet, og vi har modtaget jeres Metadata URL, foretages opsætningen og I kan benytte jer af AD FS.